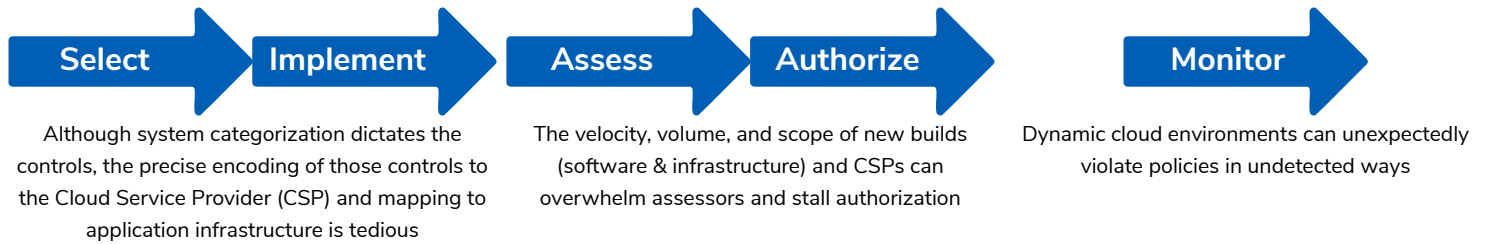


# Graphion™ | Map Every Threat. Secure Every Connection.

## Risk Management Framework (RMF) / Authorization to Operate (ATO)



**37% of compliance audits fail**

due to poor control implementation  
- State of Cloud Security Report 2025




**At least 2x more time**

needed to achieve authorization without RMF automation  
- FedScoop

**74 more days**

to identify & contain an operational issue without security automation  
- IBM Security Report

It's no secret that the Authorization to Operate (ATO) process is often slow. But CI/CD practices, complex multi-cloud systems, and evolving security threats have made it exceedingly difficult. The tailoring of controls in the selection phase is often done in a uniform manner which can result in either excessive protection or insufficient security; and with threats and technology constantly evolving, control selection should not be a one-time activity. Control implementation may differ from what's documented (especially over varying CSPs), creating misalignment that becomes evident during assessments. Coupled with inadequate assessment expertise to cover the scope and velocity of change, problems become amplified. Continuous monitoring requires ongoing assessment, vulnerability management, and risk response; but ever-changing environments and new technologies present major challenges to consistent risk tracking. A fresh approach is necessary.

 <b>Challenge</b>	 <b>Description</b>	 <b>IMPACTS TO ATO PROCESS</b>
<b>1 Development &amp; Engineering vs. Security</b>	Application teams operate under a "build now, secure later" mindset, focused of getting things to work. Conversely, Security understands the end goal of compliance, but they are often unaware of technical details and their impact on security controls.	<ul style="list-style-type: none"> <li>Establishes adversarial relationships within the "team", which only gets worse with each iteration of the rework cycle (Security continuously sends discovered vulnerabilities back to Development for resolution).</li> <li>Each rework cycle multiplies the workload for all parties, extends the timeline for ATO, and increases pressure.</li> <li>Treating security as an afterthought leads to wasted effort (developing insecure features that need to be redone) and sunk costs</li> </ul>
<b>2 Complex Control Implementation in Dynamic Clouds</b>	The intricate interconnectedness of dynamic cloud infrastructure across multiple CSPs makes it difficult to implement the right controls the right way in the right spots.	<ul style="list-style-type: none"> <li>Incorrectly implemented controls collect the wrong data.</li> <li>Wrong data can lead to a false sense of security.</li> <li>The detection and correction of incorrect control implementation takes deep expertise and time</li> </ul>
<b>3 Lack of a Fresh Repo of Control Data</b>	It takes considerable effort to gather all the relevant data for Security to assess. By the time that's done, a new build may be ready. Security is constantly chasing Development.	<ul style="list-style-type: none"> <li>Data gathering requires security control expertise and takes time to perfect.</li> <li>Time to gather the data results in delays for analysis, feedback, and corrective measures.</li> <li>The queue of builds to analyze increases process complexity, time, and the potential for errors.</li> </ul>
<b>4 Time-Consuming Assessments</b>	Once all the data is in place, Security must run their analytics, evaluate the results, and prepare direction (in detailed technical terms) for the Development Team.	<ul style="list-style-type: none"> <li>Delayed analysis increases ATO duration.</li> <li>Uncoordinated moving parts leads to frustration, morale problems, and quality issues.</li> <li>The translation of security issues into detailed development actions is error prone, negatively impacting quality and additional repair cycles</li> </ul>
<b>5 Deploy &amp; Forget</b>	Once an ATO is granted, the application is deployed and then forgotten (at least partially) until the next ATO cycle.	<ul style="list-style-type: none"> <li>Security issues go unaddressed in Production, which could be catastrophic.</li> <li>The team incurs an unknown amount of security-related debt.</li> <li>If the application survives until the next ATO cycle, the debt must be paid at that time</li> </ul>

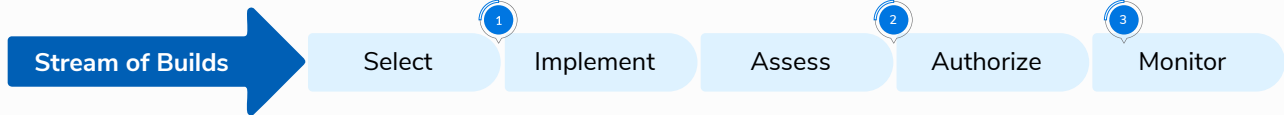
# Where to Focus

## Fully Assess at the Speed of Build

CoreStack's solution improves the quality and efficiency of the ATO process by taking a 3-pronged approach: (1) Factors in each **application's context**, aligning security controls with the unique application environment and its layers prior to assessment - thus ensuring higher value from each assessment and fewer re-runs. (2) Decreases **attack surfaces & depth** by encoding all major compliance standards and the underlying security controls for each CSP, automatically evaluating each build against those controls to detect security issues and their connectedness. (3) Uses Cloud Security Posture Management (CSPM) to extend the **continuum of risk management** by monitoring deployed applications, checking them against the relevant compliance standards, reporting policy violations, and auto-remediating issues where possible.

### Objectives

- 1 Improve the quality of assessments by putting the right controls in the right layers
- 2 Reduce assessment & authorization times while increasing accuracy
- 3 Identify, report, and correct issues after authorization/deployment



By helping teams improve the selection and alignment of security controls with a cloud application's environment, CoreStack's solution **improves the quality of the assessment**, thus **reducing rework by pinpointing issues** as early as possible. Furthermore, after builds are deployed, CoreStack **continues to find, report, and correct** issues which surface in runtime environments.



### Solution Capability



### Description

#### Holistic View (SBOM + IBOM)

Overlays each application's software on dynamic cloud infrastructure, showing the full scope of what runs on each component in the cloud ecosystem

#### Compliance Standards

Encodes security controls for all major compliance standards (e.g., NIST SP 800-53) in the language (APIs & tools) of all major CSPs

#### Compliance Posture

Reports and maintains the detailed and summarized results of each relevant Compliance Standard's run

### RMF Support

- **Select**
- **Implement**
- **Assess**
- **Authorize**
- **Monitor**

Place the right controls in the right layers

View control results for each component in the context of the application

Continue to gather, analyze, and respond to control metrics

Leverage the precise pre-mapping of controls to one or more policies

Confirm proper mapping and implementation of the right controls

Configure frequent evaluation of deployments against proper standards

Gain insights prior to assessments; configure/tune auto-remediation steps as necessary

Glean knowledge from the analysis of control results with respect to each relevant standard

Continue compliance analysis and perform auto-remediation steps

**CoreStack's solution starts at the selection & mapping of security controls and continues through runtime analysis**

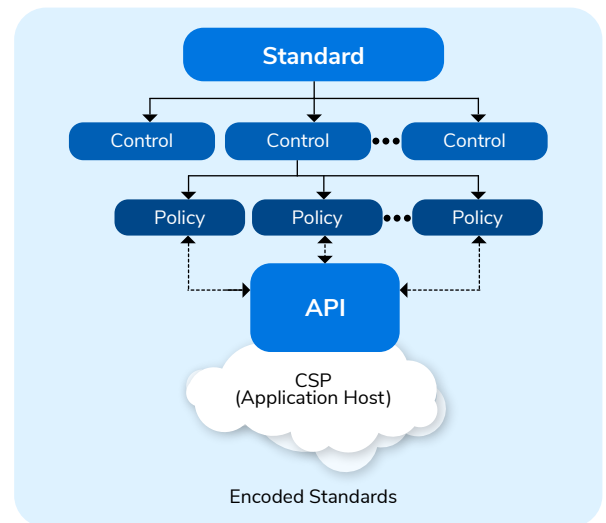
# Graphion helps your organization meet key objectives of the RMF steps, facilitating ATO issuance and subsequently maintaining the necessary security posture.

## Select

Through the presentation of an application's unique ecosystem of software and infrastructure, CoreStack helps security engineers **tailor the baseline** of security controls to address the specific needs and risks of the organization and information system. Consequently, the team can avoid the pitfalls of excessive protection (which increases costs and complexity) and insufficient security (which increases risks). Furthermore, CoreStack's presentation of each holistic system helps teams **allocate controls** by aligning those controls with the application's unique environment and its architectural layers.

## Implement

Our solution helps teams **document control implementation** by providing accurate and continuously refreshed descriptions of an application's complete ecosystem (software, infrastructure, and the combination thereof). Furthermore, CoreStack captures the detailed mapping between policies, controls, and compliance standards – as well as the results of each control assessment against a specific version of an application.



## Assess

Through the automated and frequent evaluation of controls against an application's dynamically-constructed software and infrastructure, CoreStack provides objective and precise **control assessments**. The results of these assessments provide the necessary body of evidence and artifacts for authorization. Additionally, the solution accommodates **remediation actions** on an automated basis (as scripts built from templates) and via guidelines for manual steps. By using these techniques, the team can address security concerns prior to authorization or develop POA&MS for deficiencies that cannot be remediated immediately.

## Authorize

By providing summary results of any supported (and executed) policy standard as well as the underlying detailed evaluation data for each control, build, and infrastructure mod, CoreStack support the **authorization decision** process.

## Monitor

Graphion conducts **Ongoing Assessments** for each application in two key ways: (a) for each software build, upon a CI/CD pipeline's SBOM submission; and (b) for each infrastructure modification identified via frequent CSPM runs. Through these assessments, CoreStack supports continuous **Vulnerability Management**, scoring detected issues in the context of the application and presenting risk-prioritized vulnerabilities to the team for remediation.

<b>FedRAMP High</b> Federal Risk and Authorization Management Program, HIGH FedRAMP High Baseline	<b>FedRAMP Moderate</b> Federal Risk and Authorization Management Program, MODERATE FedRAMP Moderate Baseline
<b>HIPAA</b> Health Insurance Portability and Accountability Act (HIPAA) HIPAA	<b>ISO 27001</b> Information technology   Security techniques   Information security management... ISO
<b>NIST SP 800-53 Rev. 4</b> National Institute of Standards and Technology NIST	<b>NIST SP 800-53 Rev. 5</b> NIST SP 800-53_r5 - Security and Privacy Controls for Information Systems a... NIST

Supported Compliance Standards (Sample)

# Achieving ATO Speed While Improving Security

## Rapidity

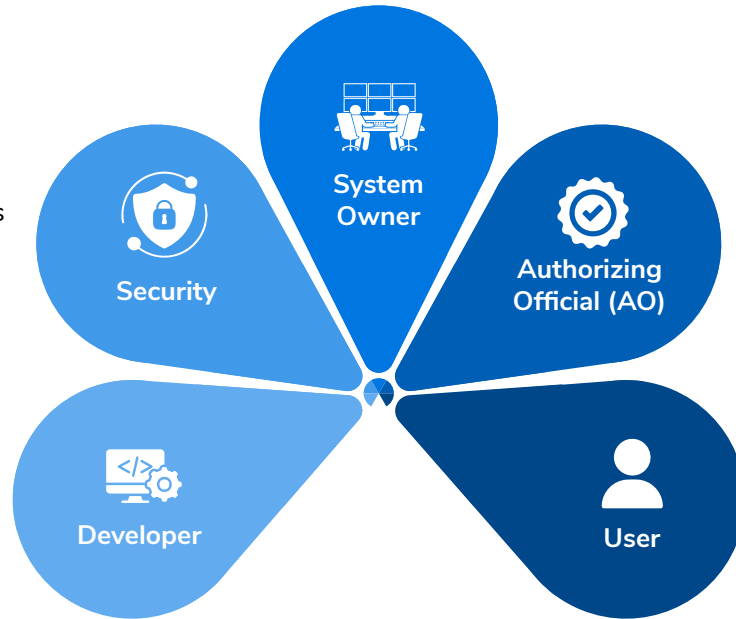
I am certain we have the right balance of security and usability, as well as a comprehensive means to oversee proper continuous risk management.

## Specificity

Even in a dynamic environment, I can conduct a self-assessment and quickly determine the effectiveness of security controls in my systems to decrease attack surfaces and depth.

## Priority

Now I clearly understand what I need to fix in my code with respect to the context of the application, even prior to assessments by the Security Team... so that we can achieve ATO as quickly as possible.



## Auditability

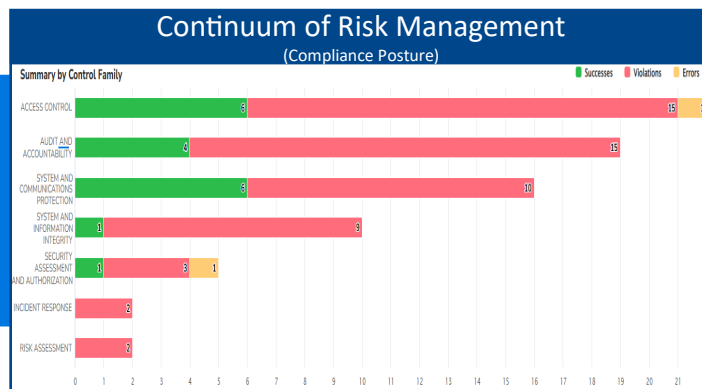
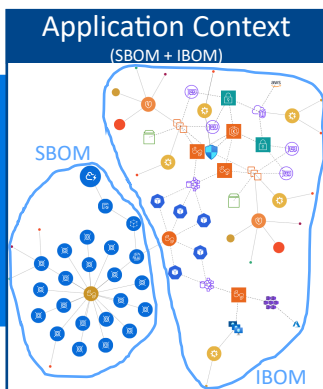
We're tracking every build's software and infrastructure, as well as ad hoc changes in the cloud... while automatically assessing those changes against the appropriate compliance standards. I'm much more confident when issuing an ATO.

## Functionality

I'm able to start using new and updated features much sooner – and am more assured the application and its data are protected.

Graphion provides detailed control information for software and infrastructure, which helps rapidly achieve ATO... respective of build velocity & volume

## Graphion's Effectiveness (examples)



CoreStack is an AI-powered NextGen Cloud Governance & Security Platform that enables enterprises to embrace cloud with confidence, rapidly achieving continuous and autonomous cloud governance at scale. CoreStack helps 750+ global enterprises govern more than \$2B in annual cloud consumption. The company is a Microsoft Azure (Legacy) Gold Partner, Amazon AWS Technology Partner with Cloud Operations Competency, Oracle Cloud Build Partner, and Google Cloud Build Partner.